Remarks:

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. The Claims have been renumbered at the request of the Examiner. The new claims numbers shall be used when referring to the claims in the amendments above and the discussion below. Claims 1 – 23 remain in the application. Claims 1, 6, 8, 16, 17, 22, and 23 are amended.

ARGUMENT

Claim 5 is rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. This rejection is respectfully traversed and Claim 5 is believed allowable based on the following discussion.

On pages 9-10 of the specification, splicing is described:

> "For example, if the message from the OEM contains BIOS-executable code, BIOS 22 can ***splice*** the code into its normal execution path, thus effectively modifying itself or *erasing* part of itself in response to the message. This "splicing" approach is better suited for controlling system features such as number of processors or memory sizes."

It will be apparent to one of ordinary skill in the art that ***splicing*** *the content of the message into an execution path of the BIOS* is an effective method to alter or modify the BIOS so it contains the desired instructions. Claim 5 requires that the splicing comprises *at least one of modifying the BIOS or erasing a portion of the BIOS, in response to the message*. It will be apparent to one of ordinary skill in the art that splicing operations may insert data (code) into an existing code, or overwrite a part of the code with the new data (code), or both. Writing over code effectively erases it, as that code will no longer be in the execution path. In some cases, the message content may request that a portion of BIOS code be erase without overwriting it. The claim requires that the content of the message be spliced into an execution path of the BIOS. In other words, the BIOS is to be modified by the message. In this case, the message may include replacement or additional code to be spliced into the BIOS code. In the case where the code from

the message is to replace some code in the BIOS, the replaced code is ***erased***, or overwritten. Thus, the limitations of Claim 5 are described in the specification (pages 9-10) sufficient to be understood by one of ordinary skill in the art.

Claims 1-4, 6-15, 16-20 and 22-23 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,463,537 to Tello (hereinafter "Tello"). This rejection is respectfully traversed and Claims 1-4, 6-15, 16-20 and 22-23 are believed allowable based on the above amendments and following discussion.

With regard to Claims 1, 8 and 17, the Examiner asserts that Tello teaches *receiving, at a BIOS, a message from an authorized party; authenticating the message; and controlling a state of a feature of a system resource, using the BIOS, according to the message*. The claims are amended to require that ***the message comprises information to determine the optional feature***. Tello teaches that a personalized computer with a unique encrypted digital signature will not boot up or recognize any data storage or communication peripheral devices without a matching personalized smart card containing a complementary encrypted digital signature. The smartcard contains an authenticating identifier. The system of Tello matches the identifier in the smartcard with the security system. Communication is synchronized between the inserted smart card and the security engine as occurs every time a smart card is inserted in the smart card reader. Next, hash numbers are read from the smart card the hash numbers are read from the security engine flash memory. The smart card hash numbers are then compared to the security engine's hash numbers. If the hash numbers in the smartcard and security engine memories do match, the security engine microprocessor **reads the security configuration parameters from the flash** memory and all allowed peripheral devices are enabled.

In contrast, the claimed invention relates to enabling optional features on a computer based on authorized ***messages*** received by the BIOS. The recited invention requires the receipt of a message, where the message defines the optional parameters. Tello does not teach or suggest that the BIOS receives messages or any communication from an authorized party. Tello teaches that a smartcard is used to decrypt and authenticate a digital signature which allows a computer to boot. The system, as taught by Tello, does not receive a message, but reads hash numbers from the smartcard. Further, once there is a match, the information defining the allowed peripherals is read from flash memory, not from the incoming message. Thus, Tello

fails to teach or suggest all of the recited elements of Applicant's invention and Claims 1, 8, 17 and their progeny are believed allowable.

As for Claims 2, 12 and 18, the Examiner asserts that Tello teaches *verifying an identifier in the message against a unique system identifier of the system*. Tello teaches identifying the purpose and type of the smartcard. Tello does not teach or suggest a unique system identifier, and further, does not teach or suggest a message having an identifier to compare to the unique system identifier. Tello does not teach any message communication, but merely reading data in the smartcard and application of the data to authorize boot and data access. Specifically described at the cited reference, Tello teaches that the flash memory of the microprocessor has a secret identifier. However, Tello teaches that the identifier is 'the same for all motherboards." [Col. 9, lines 20-30] Thus, Tello teaches away from a "***unique system identifier of the system***" as recited in Claims 2, 12 and 18. Thus, Claims 2, 12, 18 and their progeny are believed allowable.

As per Claims 3, 13 and 19, the Examiner asserts that Tello teaches *writing the message into a secure non-volatile location*. Tello does not teach or suggest receiving messages, but merely checking static data within a smartcard. Thus, Tello cannot teach writing a message that is not received. Further, the cited reference describes a command sent to the BIOS to display configuration set up screen. This command is not the same as receiving a message by the BIOS, ***wherein the message comprises information to determine the optional feature, and wherein the message further comprises a digital signature***. Moreover, the user input to the set up screen is not the same as a message having a digital signature. Tello teaches that the user input is written to CMOS, but does not verify that the input is authenticated. The claimed invention requires that a received message is authenticated before being written to a secure non-volatile location. Thus, Claims 3, 13, 19 and their progeny are believed allowable.

As for Claims 4, 14 and 20, the Examiner asserts that the remote storage is taught by Tello. However, since Tello does not teach all of the recited elements of Claims 4, 14 and 20 (see discussion above), the location of Tello's remote storage is moot, and Claims 4, 14, 20 and their progeny are believed allowable.

As for Claims 6, 16, and 22, the Examiner asserts that Tello teaches *loading and executing the content of the message using the BIOS at run-time*. Tello does not teach or suggest

receiving messages, but merely checking static data within a smartcard. Thus, Tello cannot teach loading and executing the content of the message that is not received. Further, Claims 6, 16 and 22 require that the message is received via a network transmission. In contrast, Tello requires a smartcard to be inserted in the system and does not teach or suggest receiving a message from a remote system via a network. Thus, Claims 6, 16 and 22 are believed allowable.

As for Claims 7, 15 and 23, the Examiner asserts that Tello teaches updating a feature set of the system BIOS according to the message. A feature set is defined in the specification as where status of the system features are recorded. [Page 5, lines 22 et seq.] The cited reference does not teach updating a feature set of the system BIOS, but merely teaches that allowed peripherals are loaded. Further, Claims 7, 15 and 23 are believed allowable as being dependent from allowable claims.

Claims 9 and 10 are believed allowable, at least, because they are dependent on an allowable Claim.

As for Claim 11, it has been discussed above with respect to Claims 2, 12 and 18 that the cited references of Tello do not teach storing a ***unique system identifier accessible by the BIOS***. Thus Claim 11 is believed allowable.

Claim 21 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello further in view of U.S. Patent 6,584,561 to Merkin (hereafter, "Merkin"). This rejection is respectfully traversed and Claim 21 is believed allowable based on the foregoing and following discussion.

Merkin et al. disclose a system and method for restricting a compact disk (CD) containing boot software to work only on computer systems for which the boot software has been authorized to operate. Merkin et al. do not teach or suggest *splicing the contents of a message into the BIOS execution path*, as recited in the claims. Merkin et al. disclose that a computer system is checked for predetermined identification criteria to allow boot software from a CD to run on the computer system. Merkin et al. teach that a computer system may boot using the boot software on the CD. At no time do Merkin et al. disclose that a message is sent or that the contents of the message are used to alter a portion of the existing BIOS during boot. Instead, Merkin et al. teach a system where the system is booted using the entire boot software on the CD, not contents of a message. Merkin et al. teach replacing the existing boot software (BIOS) with the software on the CD to provide new boot software (Col. 2, lines 34-38). New boot software replaced in its entirety is not

the same as ***splicing*** contents of a message into an execution path of the BIOS. Thus, Claim 21 is believed allowable.

Claim 23 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello further in view of U.S. Patent 6,769,059 to Qureshi (hereafter, "Qureshi"). This rejection is respectfully traversed and Claim 23 is believed allowable based on the foregoing and following discussion.

Qureshi et al. teach a system and method for updating a video BIOS independently of the system BIOS. This concept is not related to Applicant's claimed invention. Claim 23 requires the update of a feature set of the BIOS according to the content of the message. Qureshi et al. teach that the computer system must be powered off before the video BIOS can be updated. The video BIOS update is initiated by a hot sequence of keys. In contrast, Applicant's claimed invention uses contents of a message to update a feature set of the system BIOS. As defined, at least on page 10 of the specification, a feature set is used for multi-processor systems and comprises an MPS (Multiple Processor Specification) table for storing features related to the multiple processors, e.g., number of processors, processing speed of each of the processors, and so forth. Qureshi et al. do not teach multi-processor systems. One of ordinary skill in the art understands that including a graphics processor chip on a computer system does not make it a multi-processor system using a feature set to define the features of the various processors. Further, even if one considers a computer system having a central processor and a video/graphics processor to be a "multi-processor" system, Qureshi et al. fails to disclose or suggest updating a feature set of the system BIOS based on content of a message. All claims remaining in the application are now allowable.

CONCLUSION

In view of the foregoing, Claims 1 to 23 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 6/20/05

Joni D. Stutman-Horn
Patent Attorney
Intel Corporation
Registration No. 42,173
(703) 633-6845

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026